



NASA Standard Operating Procedure

Procedures for Agency IT Security Incident Classification and Reporting

ITS-SOP-015

Version: 20051005

Effective Date: 20051005

Expiration Date: 20071005

Responsible Office: V / Chief Information Officer

REVISION RECORD

[illegible]

Procedures for Agency IT Security Incident Classification and Reporting

Objective: In the fast-paced and challenging environment in which IT security professionals must operate, quick access to actionable data is a must. In order for this to be realized, a common classification framework and reporting hierarchy for ITS incidents is necessary. A common Agency-wide approach will enhance NASA's ability to identify, track, respond, and learn from ITS incidents.

Reference: NASA CIO directive letter, dated December 2, 2004, Subject: Information Technology Security (ITS) Incident Reporting Requirements, provides direction on the reporting of NASA ITS incidents. OMB policy requires agency procedures be consistent with guidance issued by NIST when such is available. This guidance is provided by NIST Special Publication (SP) 800-61, Computer Security Incident Reporting Guide.

Process:

1. IT Security Managers (ITSM's) shall report all IT security incidents at their Centers to NASIRC. Incidents are to be reported via the NASIRC incident database web site located at <https://nasirc.nasa.gov/Reports/login.jsp>.
2. Incidents reported to NASIRC are to be classified under one of the following categories:

Incident Category	Definition	Clarification
Denial of Service	An explicit attack on NASA systems that prevents or impairs the authorized use of networks, systems, or applications.	Includes only those attacks that deny service to NASA systems (i.e., inbound attack on NASA systems or packet flood affecting NASA systems that was a result of malicious code.)
Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity (e.g., mobile code) that infects hosts at NASA.	Includes infections that result in an outbound DOS attack that originates on NASA networks and attacks an external party.
Unauthorized Access	A person gains logical or physical access without permission to a NASA network, system, application, data, or other resource.	The emphasis is on human intervention that enables access, therefore, this category doesn't include malicious code that gains system or user privileges. These attacks should be further categorized as: <ul style="list-style-type: none">• System Compromise• User Compromise
Misuse	A person violates acceptable computing use policies.	
Multiple Component	An incident that falls into several incident categories at once.	

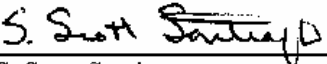
Table 1: NASA ITS Classification Framework

3. Some incidents may fit into more than one category. Centers should categorize incidents by the transmission mechanism.
 - Example 1: A virus that creates a backdoor should be handled as a malicious code incident, not an unauthorized access incident, because the malicious code was the only transmission mechanism used.
 - Example 2: A virus that creates a backdoor that has been used to gain unauthorized access should be treated as a multiple component incident because two transmission mechanisms were used.
4. For purposes of Agency-wide incident reporting, NASIRC shall group incidents in a reporting hierarchy as follows:

Occurrence	<p>The individual NASA system(s) involved in an ITS incident. The incident report should capture:</p> <ul style="list-style-type: none"> - The specific IP addresses/systems that are involved. - The total count of systems involved in an incident - Specific exploit and vulnerability <p>Example: "There were 113 reported occurrences of the Beagle Virus last quarter."</p>
Incident	<p>Comprised of one or more occurrences at a NASA Center</p> <ul style="list-style-type: none"> - Fits into one of five incident categories listed in the Classification Framework or can be categorized as a multi-component - Each Center creates a "ticket" to report the occurrences as an event in the OneNASA ITS Incident database. - The ticket details the exploit and vulnerability used against the NASA system(s). For example, "Worm/virus or unauthorized access affecting only one Center."
Event	<p>An IT security incident impacting the Agency that can be comprised of one or more related incidents at multiple Centers.</p> <ul style="list-style-type: none"> - Provides the correlation of related incidents across the Agency - Usually initiated through an Agency "call-down" <p>Example: "The MS Blaster Worm is a good example of an Agency event."</p>

Table 2 ITS Incident Reporting Hierarchy

5. Center ITSMs or a designee shall determine the incident or suspected incident's severity and potential impact on NASA's overall IT security.


 S. Scott Santiago
 Deputy Chief Information Officer
 Information Technology Security

10/5/2005
 Date